**Math 75 notes, Lectures 4 and 5**

P. Pollack and C. Pomerance

Before we focus on the specific questions raised at the end of the Lecture 3 notes, we shall discuss some further ramifications of the division algorithm for $F[x]$, where now $F$ is any field, finite or otherwise. The principal consequence is the following result.

**Theorem 1.** *If $F$ is a field, each nonzero element of $F[x]$ has a unique factorization as a product of a unit and monic irreducibles.*

Of course the uniqueness of the factorization is to be understood with the caveat that rearranging the factors does not count as a different factorization. There should also be the understanding that a single unit or monic irreducible is to be considered as a factorization with just one factor.

Here are some interesting examples. In $\mathbb{Q}[x]$ we have

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

(You should check that the two quadratics above are indeed irreducible in $\mathbb{Q}[x]$—do you know how to do that?) In $\mathbb{C}[x]$, we have

$$x^4 + 1 = (x - e^{i\pi/4})(x + e^{i\pi/4})(x - e^{3i\pi/4})(x + e^{3i\pi/4}).$$

And in $F[x]$ where $F = \mathbb{Z}/(2)$, we have

$$x^{32} + 1 = (x + 1)^{32}.$$

Why is this unique factorization theorem true? If one remembers the analogous theorem for the integers, the key step is that if a prime $p$ divides the product $ab$ of two integers $a$, $b$, then $p$ divides $a$ or $b$. This is used to show that if $p_1 p_2 \dots p_k$ is a product of primes equal to another product of primes $q_1 q_2 \dots q_l$, then the prime $p_1$ divides $q_1 q_2 \dots q_l$, and so by applying the principle repeatedly, we finally get that $p_1 \mid q_j$ for some $j$, which leads to $p_1 = q_j$. This common factor is then cancelled from the two equal products of primes, and continuing one deduces that the two lists of primes involved are identical up to order. So let us carefully prove the analogous result for irreducible polynomials.

**Proposition 1.** *If $F$ is a field, $f \in F[x]$ is irreducible, $a, b \in F[x]$, and $f \mid ab$, then $f \mid a$ or $f \mid b$.*

*Proof.* Suppose $f \nmid a$. Since $f$ is irreducible it follows that the greatest monic common divisor of $f$ and $a$ is 1. Then by the extended Euclid algorithm, there are polynomials $u, v \in F[x]$ with

$$uf + va = 1.$$

We multiply this equation by $b$, getting

$$ufb + vab = b.$$

Not too exciting yet, but now let's use that $f \mid ab$, so that we can write $ab = gf$ for some $g \in F[x]$. Thus the last equation can be rewritten as

$$ufb + vgf = b,$$

from which we can see that $f \mid b$. Indeed $(ub + vg)f = b$. □

So, that was not so hard.

One consequence of unique factorization (or Proposition 1) is the following important result.

**Proposition 2.** *If $F$ is a field, $f, g$ are different monic irreducible polynomials in $F[x]$, and $h \in F[x]$ is such that $f \mid h$ and $g \mid h$, then $fg \mid h$.*

This follows immediately from writing $h$ as a unit times a product of monic irreducibles and noticing that both $f$ and $g$ must appear in this product. But here is another proof using only Proposition 1: Since $f \mid h$, we may write $h = uf$ for some polynomial $u \in F[x]$. But the irreducible $g$ divides $h = uf$ and it does not divide $f$, since $f$ is a monic irreducible not equal to the monic irreducible $g$. So, by Proposition 1, $g \mid u$, so that $u = vg$ for some $v \in F[x]$. Thus, $h = uf = vgf$, so we see that $fg \mid h$.

Here's another important consequence of the division algorithm.

**Theorem 2.** *Suppose $F$ is a subfield of the field $K$ (that is, $F$ is a subset of $K$ closed under the plus and times of $K$ and such that $F$ is actually a field with these operations). Say $\alpha \in K$ is such that there is some nonzero $f \in F[x]$ with $f(\alpha) = 0$. Then the polynomial $f_0$ with this property of smallest degree is irreducible, and any polynomial $f \in F[x]$ with $f(\alpha) = 0$ is divisible by $f_0$. In particular, there is a unique monic irreducible polynomial (called the minimum polynomial of $\alpha$) in $F[x]$ which has $\alpha$ as a root.*

*Proof.* We first show $f_0$ is irreducible. If not, then $f_0 = uv$, where $u, v \in F[x]$ have smaller degrees than $\deg(f_0)$. We have

$$0 = f_0(\alpha) = u(\alpha)v(\alpha).$$

But, since $u, v$ have degrees smaller than $\deg(f_0)$, by the definition of $f_0$, we have $u(\alpha)$ and $v(\alpha)$ both nonzero. So, the equation just displayed cannot occur (compare with problem 3a on hw 1). Hence $f_0$ must be irreducible. To see the second part, let $f$ be any polynomial in $F[x]$ with $f(\alpha) = 0$. We divide $f_0$ into $f$ getting a quotient and a remainder:

$$f = qf_0 + r, \quad r = 0 \text{ or } \deg(r) < \deg(f_0).$$

We then evaluate both sides at $\alpha$, getting

$$f(\alpha) = q(\alpha)f_0(\alpha) + r(\alpha).$$

But $f(\alpha)$ and $f_0(\alpha)$ are both 0, so the equation simplifies to $r(\alpha) = 0$. But then, by the definition of $f_0$, it must be that $r$ is the zero polynomial, that is, $f_0 \mid f$. □

Here's a message to those students who have had advanced algebra: The way this last result is viewed is as follows. We have a ring homomorphism from $F[x]$ into the field $K$ given by replacing $x$ with $\alpha$. Since the range of this homomorphism is an integral domain, the kernel must be a prime ideal, and so must be of the form $(f_0)$ for some irreducible polynomial $f_0$ (since the hypothesis says the kernel is not just 0).

**Back to finite fields**

With these general tools we can begin in earnest our classification of finite fields. Our first result is already known to you as Fermat's little theorem in the case $F = \mathbb{Z}/(p)$, with $p$ prime, and is a consequence of Lagrange's theorem for finite groups (for those who have had group theory).

**Theorem 3.** *If $F$ is a field with $q$ elements, then $\alpha^q = \alpha$ for all $\alpha \in F$.*

*Proof.* The result is true for $\alpha = 0$, so take some $\alpha \in F$ with $\alpha \neq 0$. Consider the linear polynomial $\alpha x$. This can be viewed as a function from $F$ to $F$, and note that this function is one-to-one (injective). Indeed, if $\alpha\beta_1 = \alpha\beta_2$, then multiplying both sides by $\alpha^{-1}$ gives us that $\beta_1 = \beta_2$. It is also onto (surjective), since if $\gamma \in F$ is arbitrary, note that $\alpha^{-1}\gamma \in F$, and $\alpha$ times this is $\gamma$. (Or, one could note that any one-to-one function on a finite set to itself has to be onto.) Since the function $\alpha x$ takes 0 to 0, it follows that by removing 0 from $F$, the function is still one-to-one and onto (a bijection). In particular (where we use the notation $F^*$ to denote the set of nonzero elements of $F$),

$$\prod_{\beta \in F^*} \beta = \prod_{\beta \in F^*} (\alpha\beta). \tag{1}$$

(Note that the $\prod$ notation is just like $\sum$, but you multiply the terms instead of add them.) Do you believe this equation? The left side of (1) is the product of all of the elements of $F^*$. But the elements $\alpha\beta$ also run over all the elements of $F^*$ as $\beta$ does, since we've seen the function $\alpha x$ is one-to-one and onto. Since multiplication is commutative and associative, it follows that the two products are equal, as asserted.

Now let's say $\gamma$ is this common value in (1), and rewrite the right side of (1) as

$$\alpha^{q-1} \prod_{\beta \in F^*} \beta = \alpha^{q-1}\gamma.$$

Thus, $\gamma = \alpha^{q-1}\gamma$, and so multiplying by

$$\gamma^{-1} = \prod_{\beta \in F^*} \beta^{-1},$$

we get $\alpha^{q-1} = 1$. Multiplying by $\alpha$ gets us $\alpha^q = \alpha$, which is what we wanted. □

**Corollary 1.** *If $F$ is a finite field with $q$ elements, then the polynomial $x^q - x$ factors completely over $F$, in particular,*

$$x^q - x = \prod_{\beta \in F} (x - \beta).$$

*Proof.* It follows from Theorem 3 that each element $\beta \in F$ is a root of $x^q - x$. But $x - \beta$ is the minimum polynomial of $\beta$, so that by Theorem 2, each $x - \beta \mid x^q - x$. And so, by Proposition 2, we have that the product $\prod_{\beta \in F}(x - \beta) \mid x^q - x$. But this product has degree $q$ and is monic, just as $x^q - x$ is. Thus, they are equal. □

We are now ready to prove a wonderful consequence of the results in this lecture and the prior lectures.

**Theorem 4.** *If $F$ is a finite field with $q$ elements and $f \in F[x]$ is monic irreducible of degree $d$, then*

$$f(x) \mid x^{q^d} - x.$$

*Proof.* Say $f(x) = c_d x^d + c_d x^{d-1} + \cdots + c_0$, where each coefficient $c_i \in F$ and $c_d \neq 0$. Let $K$ denote the finite field $F[x]/(f)$. Then $K$ has $q^d$ elements. Further, we may view $F$ as a subfield of $K$, since the equivalence classes $[c]$ in $F[x]/(f)$, where $c \in F$, form a subset of the field $K$ that is closed under the operations of $K$ and is really identical to the field $F$ except that brackets appear around each element. Well, hey, it is only notationally different, so it is perfectly justified to view $F$ as a subfield of $K$. In particular, by putting brackets on the coefficients and using a new letter for the variable:

$$[c_d]t^d + [c_{d-1}]t^{d-1} + \cdots + [c_0],$$

we may now think of $f$ as a polynomial in $K[t]$ with coefficients in the subfield that we've identified with $F$. We use a new variable, since now the letter "$x$" is identified with the specific equivalence class $[x]$ of $K$. Call this special equivalence class $\alpha$, so $\alpha = [x]$ in $K$. Since $[ab] = [a][b]$ and $[a] + [b] = [a + b]$, we have

$$f(\alpha) = f([x]) = [c_d][x]^d + [c_{d-1}][x]^{d-1} + \cdots + [c_0] = [c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0] = [f(x)].$$

But in $K = F[x]/(f)$, we have $[f(x)] = [0]$. We conclude that $\alpha$ is a root of $f$. Thus, by Theorem 2, for any polynomial $g \in F[x]$, if $g(\alpha) = 0$, then $f \mid g$. But by Theorem 3, $\alpha$ is a root of $x^{q^d} - x$. Thus, $f(x) \mid x^{q^d} - x$, and we are done. □

Here is a consequence of what we have been doing that really underlines an important property of finite fields.

**Corollary 2.** *If $F$ is a finite field and $f \in F[x]$ is a monic irreducible polynomial, then over the field $K = F[x]/(f)$, the polynomial $f$ factors completely into monic degree-1 polynomials.*

*Proof.* Say $F$ has $q$ elements and $f$ has degree $d$. By Theorem 4 that $f(x) \mid x^{q^d} - x$. But by Corollary 1, $x^{q^d} - x$ factors completely into linear factors over $K$. Thus, by unique factorization of polynomials with coefficients in the field $K$, we have that $f$ also factors completely into linear polynomials over $K$. □